クラウド型 Web Application Firewall（ WAF ）

攻撃遮断くん

サーバセキュリティタイプ サービス仕様書

Ver. 2.4.0

株式会社サイバーセキュリティクラウド

変更履歴

変更日	版数	変更目的・変更箇所
2022年11月1日	2.0.0	初版作成
2022年11月15日	2.0.1	4.9. 動作環境 ・サポート対象OSに「MIRACLE LINUX 8」を追加
2023年1月18日	2.0.2	4.10 通知メール一覧 ・内容を更新
2023年3月8日	2.1.0	全体 ・エージェントの主要構成ファイルのパスを変更 ・その他、細かい修正
2023年4月6日	2.1.1	4.9. 動作環境 ・サポート対象OSに「Rocky Linux 9」「RedHat Enterprise Linux 9」を追加
2023年5月31日	2.2.0	3.2.1. プロフィール情報 ・メールアドレスの説明を変更 3.9. 設定変更履歴 ・項目追加 3.10.4. ユーザーメニュー ・操作権限を更新 3.14.3. ユーザーメニュー ・操作権限を更新 3.7.1.2. WAF詳細設定 ・除外IPの記述を更新 4.9. 動作環境 ・サポート対象OSに「Amazon Linux 2023」を追加
2023年6月7日	2.2.1	3.5.2. CSVダウンロード ・項目追加 3.10.2. ユーザー管理 ・二段階認証の表示を追加 3.8.1. エージェント一覧 ・絞り込み条件に「ホストキー」を追加
2023年6月14日	2.2.2	3.8.3. エージェント編集 ・項目名変更および追加
2023年8月16日	2.2.3	4.9. 動作環境 ・サポート対象OSに「Debian12」「MIRACLE LINUX 9」を追加
2023年9月6日	2.2.4	3.13. 設定制限値一覧 ・ユーザー（登録数）の制限値を変更
2023年9月27日	2.2.5	3.14.3.ユーザーメニューの操作権限 ・「お問い合わせ」を追加
2024年1月11日	2.2.6	3.7.1.2. WAF詳細設定 ・ルール一覧画面の絞り込み条件を追加 3.8.1. エージェント一覧 ・ステータス総数表示の説明を追加 4.9. 動作環境 ・NginxおよびModSecurityの動作検証バージョンを更新
2024年5月1日	2.2.7	3.10.2. ユーザー管理 ・CSVダウンロード機能の説明を追加

2024年5月22日	2.2.8	4.9. 動作環境 ・サポート対象OSのEOLポリシー項目を追加
2024年6月12日	2.2.9	4.9. 動作環境 ・サポート対象OSに「Ubuntu 22.04」を追加 ・その他、細かい修正
2024年11月13日	2.2.10	2.2. 提供機能一覧 ・内容を一部更新 3.5.1. 条件を指定して絞り込み ・絞り込み条件の項目を変更 3.7.1.1. WAF設定新規作成 ・攻撃検知メールの本文を修正
2025年1月22日	2.2.11	4.9. 動作環境 ・サポート対象OSに「Windows Server 2025」を追加
2025年2月7日	2.3.0	3.2.4. ライセンス情報 3.11. 契約管理（代理店アカウント用メニュー） ・API機能に関する記載を追加 5. 留意事項 ・新規項目を追加
2025年4月30日	2.3.1	3.3.1. 攻撃検知状況 ・内部データベースに関する記述を削除
2025年6月18日	2.3.2	3.1.2. 表示モード ・新規項目を追加
2025年7月16日	2.3.3	3.14. 設定制限値一覧 ・「カスタムルールの登録数」を適切な表現に修正
2025年8月6日	2.3.4	3.2.1. プロフィール情報 3.10.2. ユーザー管理 ・メール通知カテゴリの説明を追加
2025年9月17日	2.3.5	4.9. 動作環境 ・サポート対象OSに「RedHat Enterprise Linux 10」「Alma Linux 10」「Rocky Linux 10」「CentOS Stream 10」を追加 ・サポート対象OSのEOLポリシーについて注釈を追記
2025年11月12日	2.3.6	4.9. 動作環境 ・サポート対象OSのEOLポリシーについて修正
2025年11月26日	2.4.0	3.4.2. 月次レポート ・新規項目を追加 3.6. レポート ・ダウンロード手順を追加 その他、細かい修正

目次

1. 本書について

1.1. はじめに

本書では「攻撃遮断くん サーバセキュリティタイプ」（以下、本サービス）のサービス仕様を定めます。

1.2. 本サービスの概要

本サービスはWebアプリケーションへの攻撃に対して、検知・防御を行うセキュリティ対策製品です。
本サービスはお客様Webサーバの前面に配置して通信を解析し、Webサイトを保護する機能をクラウド上で提供します。

1.3. 用語

本書において使用する用語の定義を次のとおり定めます。

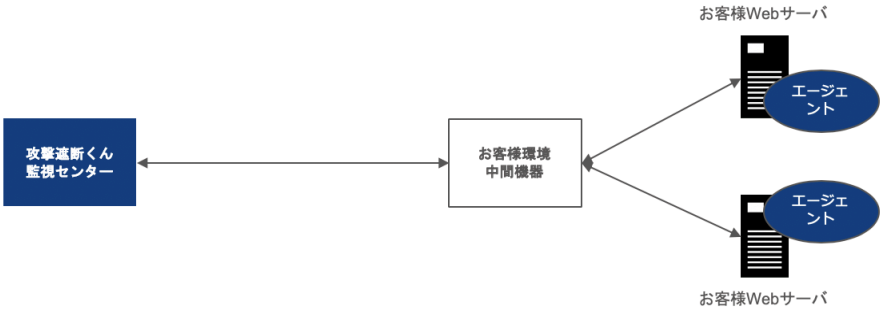
用語	用語の定義
本サービス	● 「攻撃遮断くん サーバセキュリティタイプ」
本書	● 「攻撃遮断くん サーバセキュリティタイプ サービス仕様書」
WAF	● Web Application Firewallの略称 ● Web アプリケーションへのサイバー攻撃を検知・遮断し、Web サイトを保護する機能
契約者	● 本サービスの利用に際し当社と利用契約を締結される企業・組織・団体
お客様	● 契約者を含む本サービスの利用者
エージェント	● お客様 Webサーバ内で稼働するWAF制御プログラム ● Webアプリケーションに対する各情報を収集、監視センターと連動して動作する ● 監視センターからの制御指示を元に攻撃対象の通信を遮断する制御を行う
監視センター	● 当社で管理するWAF制御システム ● エージェントが収集した各種情報を元に攻撃種別や脅威レベルの判断を行い、エージェントに対して条件に合致する通信の遮断制御指示を行う

2. サービス提供仕様

2.1. 提供プラン

本サービスでは3種類のプランを提供しています。

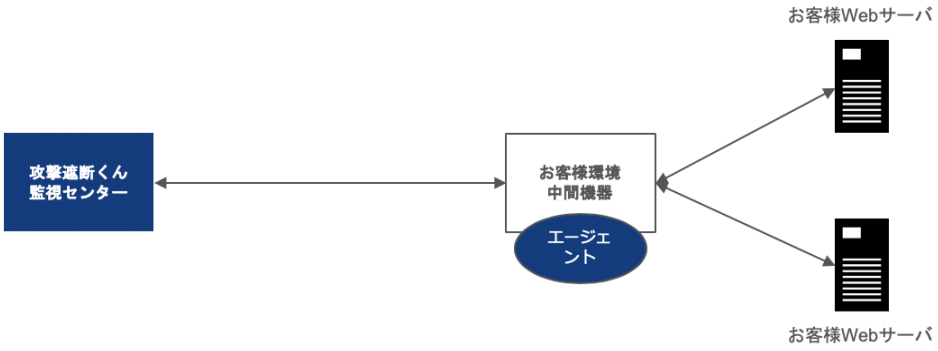
2.1.1. ベーシックプラン



お客様 Webサーバにエージェントをインストールし、ご利用いただくプランです。
1サーバOSごとに1エージェントを導入します。

※ 仮想環境をご利用の場合、ホストOS単位ではなくゲストOS単位でエージェントを導入します
※ ベーシックプランは導入するOS数による課金体系です
※ コールドスタンバイ方式のサーバ2台に導入する場合、1契約でサーバ2台へ導入可能です
※ ホットスタンバイ方式のサーバ 2 台に導入する場合、2契約が必要です

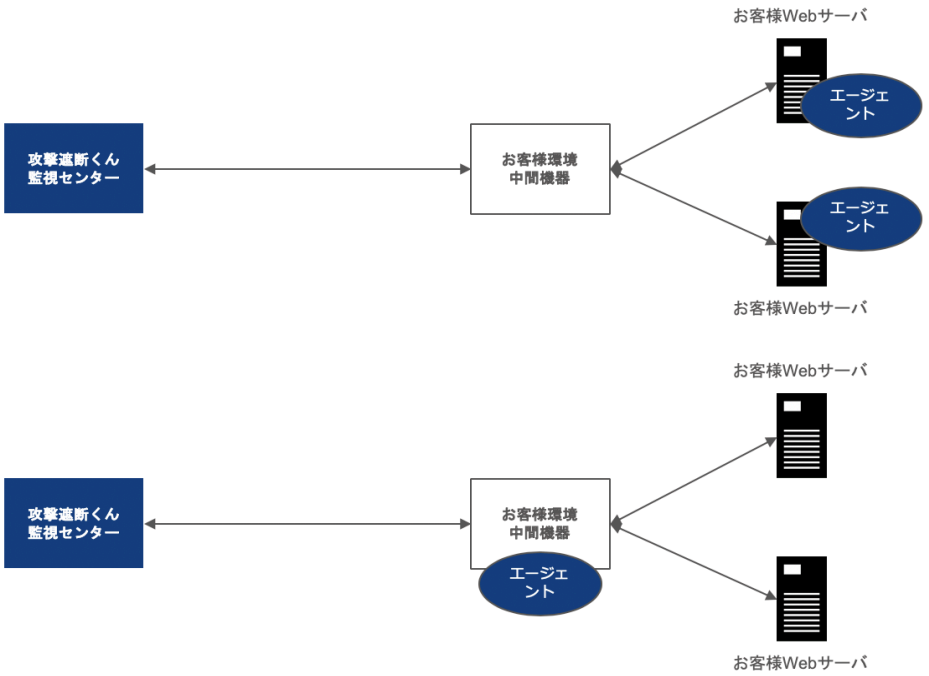
2.1.2. 従量課金プラン



お客様 Web サーバーの前段に配置しているリバースプロキシサーバーやロードバランサーにエージェントをインストールし、ご利用頂くプランとなります。
1 つのサーバー OS に 1 つのエージェントを導入していただきます。

※ 仮想環境をご利用の場合、ホスト OS 単位ではなく、ゲスト OS 単位にエージェントを導入します
※ 従量課金プランは月間のログ数による課金体系となります

2.1.3. 使い放題プラン



お客様Webサーバ/リバースプロキシサーバ/ロードバランサーにエージェントをインストールし、 ご利用いただくプランです。
1サーバOSごとに1エージェントを導入します。

※ 仮想環境をご利用の場合、ホストOS単位ではなくゲストOS単位でエージェントを導入します
※ 使い放題プランは導入するOS数に制限なくエージェントを発行可能なプランです

2.2. 提供機能一覧

本サービスにおいて提供する機能を下表に示します。

項目	概要
ダッシュボード	Webサーバーへの攻撃を24時間365日リアルタイムで確認可能です。
分析ボード	WAFで検知した攻撃を多角的に分析し表示します。
攻撃ログ	WAFで検知した攻撃情報の履歴を表示・検索できます。
月次レポート	検知レポートをダウンロードできます。
WAF設定	WAF機能の設定を複数のエージェントに対して一元管理が可能です。
エージェント管理	Webサーバに導入したWAF制御プログラムを管理できます。
アカウント管理	アカウントおよびグループを管理できます。
攻撃検知メール	WAF検知時の検知情報をメールで通知します。
サービスドキュメント	サービス仕様書・マニュアル・FAQ等のドキュメントサイトへのリンクを表示します。
サポートデスク （お問い合わせ）	QA、仕様確認、設定依頼、誤検知対応、セキュリティに関するご質問に回答します。
サイバー保険付帯	10Gbps以上のDDoS攻撃やゼロデイ攻撃により、お客様に発生した損害を補償します。

3. 提供機能仕様

3.1. 管理画面仕様

3.1.1. 動作環境

- 対象Webブラウザ
  - Google Chrome　　:最新バージョン
  - Mozilla Firefox　　:最新バージョン
  - Microsoft Edge　　:最新バージョン
  - Safari　　:最新バージョン

- Webブラウザの設定要件
  - Javascript　　:有効
  - Cookie　　:有効
  - localStorage　　:有効
  - TLS　　:TLS 1.2

3.1.2. 表示モード

管理画面右上メニュー（「アカウント設定」左のアイコン）より表示モードを選択できます。

項目	内容
ライト（デフォルト）	明るい配色（白基調）で管理画面を表示します。
ダーク	暗い配色（黒・グレー基調）で管理画面を表示します。
自動	ブラウザやOSの設定に合わせて、ライトまたはダークを自動で切り替えます。

3.2. アカウント設定

管理画面右上メニューより次の情報を表示します。

- プロフィール情報
- パスワード変更
- 請求先情報
- ライセンス情報

3.2.1. プロフィール情報

ログインユーザーの登録情報を表示・編集します。

項目	内容
契約ID	契約者固有のID情報を表示
契約者	契約者の組織名を表示
ユーザー名	管理画面に表示するログインユーザー名を表示・編集
ユーザー名（カナ）	ユーザー名の読み仮名を表示・編集
メールアドレス	ユーザー名と一意に紐付くメールアドレスを表示・編集
所属/部署	所属部署名を表示・編集
電話番号	電話番号または携帯電話番号を表示・編集
お知らせ通知メール	お知らせ通知メールの有効・無効を設定 通知対象カテゴリを「お知らせ」「機能追加」「メンテナンス情報」「障害情報」「ルール更新」「セキュリティ情報」から選択 ※ 重要なお知らせはカテゴリ選択の有無にかかわらず送信されます
ログイン通知メール	管理画面へのログインをメールで通知

二段階認証設定

Google Authenticator（iOS版 / Android版 ）を用いて管理画面ログインアカウントのセキュリティを強化します。

ログインパスワードが漏洩・盗難された場合、二段階認証を設定することでアカウントの不正使用を防止します。

3.2.2. パスワード変更

管理画面のログインパスワードを変更します。

3.2.3. 請求情報

次の請求先情報を表示します。

- 請求先宛名
- 住所
- 電話番号
- FAX番号
- 所属/部署
- 担当者名
- メールアドレス

3.2.4. ライセンス情報

所有しているライセンスキーおよびAPIキー情報を表示します。

項目	内容
ライセンスキー	発行済みのライセンス情報を一覧で表示します。 ● ライセンスコード ● プランコード ● 申込日 ● 契約期間 ● 適用中エージェント（詳細情報）
APIキー	発行済みのAPIキー情報を一覧で表示します。 ● APIキー ● メモ ● 有効期限日

※ APIキーの発行にはサポート窓口への申請が必要です。詳細なご利用方法は「利用マニュアル」を参照してください

3.3. ダッシュボード

3.3.1. 攻撃検知状況

攻撃検知状況を表示します。

項目	内容
検知状況 （数字表示）	監視センターに送信されたログ数（正常通信のログ含む）と攻撃判定したログ数を表示 ● 今日の攻撃検知状況 ● 昨日の攻撃検知状況 ● 一昨日の攻撃検知状況 ● 今月の攻撃検知状況 ● 先月の攻撃検知状況 ※「今日の攻撃検知状況」は常時「集計中」と表示されます ※ 夜間に実施される集計処理が未完了の場合「集計中」と表示されます ※ 利用開始月より以前の場合「集計中」と表示されます
検知状況 （地図表示）	・世界地図　：攻撃ログを検知順にアニメーション表示 ・攻撃日時　：攻撃ログ上の検知日時を表示 ・攻撃元IP　：攻撃ログ上の IP アドレスと国名（括弧内）を表示 ・脅威カテゴリ：検知した攻撃種別を表示 ・脅威レベル　：攻撃の脅威レベルを3段階（High / Middle / Low）表示

3.4. 分析ボード

3.4.1. 表示機能一覧

検知した攻撃情報の分析結果を表示します。

項目	内容
対象期間	分析ボード全体における表示対象期間を選択して表示 ・過去1日 / 過去1週間 / 過去1ヶ月（デフォルト） / 過去3ヶ月 ※対象ホストキーと組み合わせた選択表示も可能です
攻撃ヒートマップ	攻撃数の多い国をヒートマップ（色の濃淡）で可視化して表示
攻撃数推移（合計）	対象期間における攻撃数の推移をグラフで表示
攻撃数推移（カテゴリ別）	対象期間における攻撃数の推移をカテゴリ別にグラフで表示
攻撃カテゴリ別集計	対象期間における攻撃数をカテゴリ別に円グラフで表示
ルールID別集計	対象期間における攻撃数をルールIDごとに集計し、集計数の多い順に棒グラフで表示
攻撃元国TOP10	対象期間における攻撃数を国別で集計し、集計数の多い順に棒グラフで表示
攻撃元IP別集計	対象期間における攻撃数をIPアドレスごとに集計し、集計数の多い順に棒グラフで表示

※ 分析結果は収集したログ情報の「3ヶ月分」もしくは「10,000件」を上限として表示します

3.4.2. 月次レポート

月次レポートのダウンロードリンクを発行します。
ダウンロードリンクは管理画面上で発行するか、メールで送付するかを選択できます。
※メール送付時の宛先は、ログインアカウントに登録されているメールアドレスです

3.5. 攻撃ログ

検知した攻撃情報を表示します。

3.5.1. 条件を指定して絞り込み

指定した条件で攻撃ログを絞り込みます。

項目	内容
対象ホスト	攻撃対象のホストを指定
攻撃日時 From	カレンダーから開始日時を指定（直接入力可）
攻撃日時 To	カレンダーから終了日時を指定（直接入力可）
脅威レベル	High / Middle / Low の3種類から選択
脅威カテゴリ	カテゴリ項目から選択 ● ブラックリストUA ● ブルートフォース ● デシリアライゼーション ● HTTPインジェクション ● LDAPインジェクション ● NoSQLインジェクション ● OSコマンドインジェクション ● その他 ● Webスキャン ● サーバサイドコードインジェクション ● サーバサイドインクルードインジェクション ● サーバサイドリクエストフォージェリ ● SQLインジェクション ● ディレクトリトラバーサル ● 固有の脆弱性 ● クロスサイトスクリプティング ● XML外部エンティティ
アクション	遮断 / 検知 のいずれかを選択
攻撃元IP	攻撃元IPアドレスを指定
ルールID	検知ルールのルールIDを指定
国コード	攻撃元IPアドレスの国コードを指定（例「JP」「 US」）
表示数	攻撃ログの表示件数を選択

※ 分析結果は収集したログ情報の「3ヶ月分」もしくは「10,000件」を上限として表示します
※ 絞り込みを行わない場合は攻撃ログをすべて一覧表示します
※ 対象ホストを指定した場合は、ホスト（エージェント）ごとに「3ヶ月分」もしくは
「10,000件」を上限として表示します

3.5.2. CSVダウンロード

攻撃ログをCSV形式でダウンロードします。指定条件で絞り込みをしている場合は、絞り込み後の攻撃ログをダウンロードします。

CSVカラム

日時 | 対象ホストキー | 対象ホスト名 | 攻撃元国コード | 攻撃元IP | ルールID | ファイルパス | 脅威レベル | 脅威カテゴリ | ログ

3.6. レポート

検知内容を月次レポートとして提供します。月次レポートには次の内容が記載されます。

- 日付別攻撃ログ件数
- 攻撃種別攻撃ログ件数
- 攻撃種別割合

※ ご利用月の翌月10日頃までに月次レポートが公開されます。
※月次レポートは分析ボード＞月次レポート画面からダウンロードリンクを発行します。

3.7. サーバタイプメニュー

3.7.1. WAF設定

WAF設定の作成や確認、編集を行います。

3.7.1.1. WAF設定新規作成

新規のWAF設定を作成します。

項目	内容
共有範囲	WAF設定の管理対象ユーザーを定義 ・全ユーザー　　:すべてのユーザーが管理可能 ・グループ　　:作成者と同一グループのユーザーが管理可能 ・個別　　:作成者のみ管理可能 ※共有範囲が「個別」のWAF設定は共有設定で別途権限付与が可能です
WAF設定名	任意の設定名を入力します
遮断時間	攻撃元IPアドレスを遮断する時間を入力 （ デフォルト:600[10分間] ）
遮断モード	遮断アクションの有効/無効を選択 ・ON　：　WAFルールの遮断動作が有効になります ・OFF　：　WAFルールの遮断動作が無効（検知）になります （ デフォルト:ON ）
ルールデフォルトアクション	追加および更新ルールのアクションを定義 ・遮断　：　検知した通信を遮断 ・検知　：　検知のみ実施 ・OFF　：　何もしない （ デフォルト:遮断 ）
攻撃検知メール	攻撃検知を通知 ・通知する / 通知しない のいずれかを選択 （ デフォルト:通知する ）
オンライン/オフライン変更メール	監視センターとの接続状態の変化をメールで通知 ・通知する / 通知しない のいずれかを選択 （ デフォルト:通知する ）
攻撃検知メール通知先・ オンライン/オフライン変更メール通知先	攻撃検知メールおよびオンライン/オフライン変更メールを送付するメールアドレスを入力 ※ 複数登録は改行区切りで入力

攻撃検知メール

攻撃検知メールはWebサーバへの攻撃検知結果をWAF設定登録のメールアドレスへ通知する機能です。

項目	内容
通知先	WAF 設定にご登録のメールアドレス
送信元	alert@shadan-kun.com
件名	攻撃遮断くん攻撃検知メール -（ ホストキー ）[ホスト名] - [ルール説明]
本文	攻撃遮断くんが攻撃を検知しました。 時刻：***YYYY MM DD hh : mm : ss*** 検知したファイル：（ ホスト名 ）***IP***アドレス -> お客様環境ログのフルパス シグニチャ番号 [ルール***ID***]に該当する攻撃です -> [ルール説明] 詳細は、管理画面よりご確認ください。 https://dashboard.shadan-kun.com/ 検知したログ： ～ ログ内容 ～

※ 青字箇所は検知内容や時間帯等により変動します

留意事項

- 攻撃検知メールはすべてのメール配送を保証するものではありません。検知情報の詳細は管理画面の「攻撃ログ」を参照してください。

3.7.1.2. WAF詳細設定

「共有」ボタン

WAF設定の共有範囲が「個別」の場合に、作成者以外のユーザーにWAF設定の権限を追加します。

項目	権限
閲覧権限	WAF設定の表示
編集権限	WAF設定の表示・変更
管理権限	WAF設定の表示・変更・削除

「適用」ボタン

WAF設定内容を適用します。

監視基本設定

「3.7.1.1. WAF新規作成」で設定した内容の表示・編集を行います。

WAFルール

WAFルールの一覧表示・編集を行います。

項目	内容
ルールID	WAFで定義されたルールの識別情報を表示
脅威カテゴリ	ルールIDの脅威カテゴリを表示
脅威レベル	脅威の重要度を表示 ・High / Middle / Low の3段階で表示
詳細説明	ルールの詳細説明を表示
アクション	ルール該当時のアクションを選択 ・遮断 ： 検知した通信を遮断 ・検知 ： 検知のみ実施 ・OFF ： 何もしない （ デフォルト：遮断 ）
除外設定	特定条件に合致したリクエストをルールIDから除外 ・カスタムルール名 ：任意の設定名を入力 ・送信元IP ：除外対象IPアドレスを入力 ・URL ：除外対象URLパスを入力 ・パターンマッチ条件 ：除外対象文字列を入力 ※URLパスを含むログ全体から除外文字列をパターンマッチします

※ 送信元IPを複数指定する場合は「,（カンマ）」区切りで入力してください
【入力例】「203.0.113.1,203.0.113.2,203.0.113.3」
※ 送信元IPを範囲指定する場合はCIDR表記で入力してください
【入力例】「203.0.113.0/24」（IPアドレス範囲が「203.0.113.0 - 203.0.113.255」の場合）

WAFルール一覧画面では次のフィルタ条件で絞り込みが可能です。

- ルールID
- 脅威カテゴリ
- 除外設定

- アクション

IPリスト

信頼するIPアドレスを登録します。
登録IPアドレスからの通信はWAFルールによる検知・遮断から除外されます。

IPアドレスはCIDR表記による範囲指定が可能です。

【表記例】
- 単一指定：203.0.113.100
- 範囲指定：203.0.113.0/24（203.0.113.0～203.0.113.255）

エージェント

WAF設定の管理対象エージェントの情報を表示します。
- ホストキー
- ステータス

※ エージェント登録については「3.9. エージェント管理」を参照してください

設定配信履歴

WAF設定の履歴情報を表示します。

3.8. エージェント管理

Webサーバにインストールするエージェント情報の登録・管理を行います。

3.8.1. エージェント一覧

登録したエージェントを一覧で表示します。

項目	内容
ホストキー	エージェントの管理識別コード
ホスト名	Webサーバを識別するためのホスト情報
WAF設定	管理対象のWAF設定名
ステータス	監視センターとの接続状態 ・発行手続き中　：　エージェントキー発行前の状態 ・未接続　　：　エージェントキー発行後、接続がない状態 ・オンライン　：　監視センターと正常に接続している状態 ・オフライン　：　オンライン後、監視センターと切断した状態
詳細（アイコン）	エージェントの詳細情報とコピーリンクを表示 ・エージェントキー：エージェントインストール時に使用 ・接続情報：エージェントの設定ファイルに記載する情報
攻撃ログ（アイコン）	エージェントの攻撃ログを表示
編集（アイコン）	エージェントの編集画面に遷移
削除（アイコン）	エージェントを削除

ステータス総数

エージェント一覧画面ではステータスごとの総数が表示されます。

- 発行手続き中
- 未接続
- オンライン
- オフライン

絞り込み

エージェント一覧画面では次のフィルタ条件で絞り込みが可能です。

- ホストキー
- ホスト名
- ステータス
- メモ

3.8.2. エージェント登録

新規エージェントを登録します。

項目	内容
ホスト名	ご利用サーバを識別するためのホスト名を入力
ライセンスコード	ご契約中のライセンスコードを選択
WAF設定	管理対象のWAF設定を選択
OS種別	対象ホストのOS情報を入力（任意項目）
メモ	任意入力欄

3.8.3. エージェント編集

既存エージェントの設定を編集します。

項目	内容
ホストキー ※1	エージェントの管理識別コードを表示
ライセンスコード ※1	エージェントのライセンスコードを表示
ホスト名	Webサーバを識別するためのホスト情報を表示・編集
WAF設定	管理対象のWAF設定を表示・編集
OS種別	対象ホストのOS情報を入力
メモ	任意入力欄
監視センターホスト名 ※1	接続先監視センターのホスト名を表示
監視センターIPアドレス ※1	接続先監視センターのIPアドレスを表示
接続先ポート番号 ※1	監視センターの通信ポート番号を表示
ステータス ※1	監視センターとの接続状態を表示
エージェントキー ※1	エージェントインストール時に使用する識別子情報を表示
エージェントキー発行日時 ※1	エージェントキーの発行日時を表示

※1 表示のみの項目です（変更はできません）

3.9. 設定変更履歴

WAF設定の変更やルール更新の履歴を表示します。

※ 設定変更履歴の閲覧にはオーナー権限が必要です
※ 直近6ヶ月以内の設定変更履歴を閲覧できます

3.9.1. 条件を指定して絞り込み

指定した条件で設定変更履歴を絞り込みます。

項目	内容
変更日時 From	カレンダーから開始日時を指定（直接入力可）
変更日時 To	カレンダーから終了日時を指定（直接入力可）
操作ユーザー	ユーザー名を入力

※ 絞り込みを行わない場合は設定変更履歴をすべて一覧表示します

設定変更履歴の一覧画面では次の項目を表示します。

項目	内容
操作日時	設定変更を実行した日時を表示
操作ユーザー	設定変更を実行したユーザー名を表示
対象	対象の設定を表示
タイトル	WAF設定名やルール名を表示
操作種別	設定変更内容を表示 ・新規追加 ・更新 ・削除
詳細	設定変更の詳細を表示

3.10. アカウント管理

ユーザー・グループの管理を行います。

3.10.1. 権限の種類

本サービスでは複数のユーザーアカウント管理が可能です。
作成したユーザーアカウントはグループ化をすることで、WAF設定やエージェントに対して効率的な管理運用が可能です。

項目	実行可能な操作
オーナー	・契約情報の管理 ・全グループ , 全ユーザー管理 （追加 , 変更 , 削除） ・全WAF設定 , 全エージェント管理 （追加 , 変更 , 削除） ・グループにWAF設定権限を付与 ・お知らせの連絡先 ※1
グループオーナー	・WAF設定 , エージェント管理 （追加 , 変更 , 削除） ・ユーザー管理 （追加 , 変更 , 削除） ・ユーザーにWAF設定権限を付与 ・お知らせの連絡先 ※1
一般ユーザー	・WAF設定管理 ・エージェント管理 ・お知らせの連絡先

※1 緊急時（障害発生等）にCSCからご連絡する場合があります

3.10.2. ユーザー管理

ユーザーアカウントの管理を行います。

ユーザー一覧

登録ユーザーを一覧で表示します。

項目	内容
ユーザー名	登録ユーザー名を表示
メールアドレス	登録メールアドレスを表示
グループ名	ユーザーの所属グループを表示
二段階認証	二段階認証のON/OFFを表示
ステータス	有効 / 利用停止の2種類で表示
「編集」ボタン	ユーザー編集画面に遷移
「削除」ボタン	ユーザーを削除

新規作成 / 編集

ユーザーの新規作成・編集を行います。

項目	内容
顧客	組織名を表示
ロール	オーナー / 一般ユーザーの2種類で表示 ● オーナー　：契約者アカウント ● 一般ユーザー：オーナーが作成したアカウント
ユーザー名	ユーザーアカウントの利用者名を表示・編集
ユーザー名（カナ）	ユーザー名の読み仮名を表示・編集（任意項目）
メールアドレス	ユーザー名の登録メールアドレスを表示
所属/部署	所属部署名を表示・編集（任意項目）
電話番号	電話番号または携帯電話番号を表示・編集（任意項目）
ステータス	有効 / 利用停止の2種類で表示
お知らせ通知メール	お知らせ通知メールの有効・無効を設定 通知対象カテゴリを「お知らせ」「機能追加」「メンテナンス情報」「障害情報」「ルール更新」「セキュリティ情報」から選択 ※ 重要なお知らせはカテゴリ選択の有無にかかわらず送信されます
ログイン通知メール	ログイン通知メールの有効・無効を設定 ※ 管理画面へのログイン状況を通知します
二段階認証	二段階認証のON/OFFを表示 ※ 編集画面のみ表示します

ダウンロード

ユーザー一覧をCSV形式でダウンロードします。

権限	出力カラム
オーナー	ID,ユーザー名,ユーザー名(カナ),メールアドレス,所属/部署,電話番号
グループオーナー	
代理店	ID,顧客,ロール,ユーザー名,ユーザー名(カナ),メールアドレス,所属/部署,電話番号

※ CSVダウンロードにはユーザー作成権限が必要です
※ ユーザー一覧で表示されるユーザーが対象です（ログイン中のユーザーはダウンロード対象外）

3.10.3. グループ管理

ユーザーが所属するグループの管理を行います。

グループ一覧

登録グループを一覧で表示します。

項目	内容
グループ名	グループ名を表示
「編集」ボタン	グループ編集画面に遷移
「削除」ボタン	グループを削除

新規作成

グループの新規作成を行います。

項目	内容
顧客	組織名を表示
グループ名	グループ名を表示・編集
詳細説明	グループに対する説明を表示・編集（任意項目）

編集

作成したグループの編集を行います。

項目	内容
「編集」ボタン	グループ編集
「追加」ボタン	所属ユーザーを表示・編集
ユーザー名	所属ユーザーを表示
タイプ	グループに対する管理権限を表示 ・グループオーナー　：　グループの管理者 ・メンバー　　：　グループに所属するメンバー

3.10.4. 権限一覧

オーナーメニュー

機能	オーナー	グループオーナー	メンバー
ユーザーの閲覧	◯	◯※1	✖
ユーザーの追加 / 編集 / 削除	◯	◯※1	✖
グループの閲覧	◯	◯※1	✖
グループの編集	◯	◯※1	✖
グループの追加 / 削除	◯	✖	✖

※1 グループへの権限が必要です

ユーザーメニュー

機能	オーナー	グループオーナー	メンバー
ダッシュボード	◯	◯※1	◯※1
分析ボード	◯	◯※1	◯※1
攻撃ログ	◯	◯※1	◯※1
レポート	◯	◯	◯
WAF設定の閲覧	◯	◯※1	◯※1
WAF設定の追加	◯	◯	✖
WAF設定の編集 / 削除	◯	◯※2	◯※2
監視エージェントの閲覧	◯	◯※2	◯※2
監視エージェントの追加 / 編集 / 削除	◯	◯※2	◯※2
設定変更履歴の閲覧	◯	✖	✖
請求情報の閲覧	◯	✖	✖
プロフィール情報の閲覧 / 編集	◯	◯	◯
お問い合わせ	◯	◯	×
FAQ	◯	◯	◯
マニュアル	◯	◯	◯

※1 アカウントへの権限が必要です
※2 グループへの権限が必要です

3.11. 契約管理（代理店アカウント用メニュー）

顧客の管理を行います。

※ 本メニューは代理店アカウント用のメニューです。顧客用のアカウントでログインしている場合は表示されません。

3.11.1. 顧客管理

顧客の管理を行います。

顧客一覧

登録顧客を一覧で表示します。

項目	内容
代理店	紐づく代理店名を表示
顧客種別	顧客種別を表示 ● 一般 ● 代理店
顧客名	顧客名を表示
契約ID	顧客の契約IDを表示
ステータス	顧客の承認ステータスを表示
「編集」ボタン	顧客編集画面に遷移
「設定」ボタン	顧客の設定情報を表示

新規作成 / 編集

ユーザーの新規作成・編集を行います。

項目	内容
代理店	組織名を表示
入力項目	【必須項目】 ● 顧客名 【任意項目】 ● 顧客名(カナ) ● 電話番号 ● 郵便番号 ● 都道府県 ● 市区町村 ● 町域名・番地 ● その他住所

	● 企業サイト
オーナー	オーナー権限を持つユーザーを選択
グループ機能利用	グループ機能利用のON/OFF

設定

顧客の設定情報を表示します。

項目	内容
詳細情報	顧客の詳細情報を表示 ● 契約ID ● 代理店 ● オーナー ● 電話番号 ● 住所 ● 企業サイト
所属ユーザー	顧客の所属ユーザー情報を表示 ● ユーザー名 ● メールアドレス ● 所属タイプ
ライセンスキー	顧客が発行済みのライセンス情報を一覧で表示します。 ● ライセンスコード ● プランコード ● 申込日 ● 契約期間 ● 適用中エージェント（詳細情報）
APIキー	顧客が発行済みのAPIキー情報を一覧で表示します。 ● APIキー ● メモ ● 有効期限日

※ APIキーの発行にはサポート窓口への申請が必要です。詳細なご利用方法は「利用マニュアル」を参照してください

3.12. お問い合わせ

サポート窓口へのメール問い合わせフォームを提供します。

項目	内容
担当者名	お問い合わせ担当者名を入力

メールアドレス	お問い合わせ差出人メールアドレス(From)を入力
電話番号	ご連絡可能な電話番号を入力(任意) ※内容に応じてお電話で連絡させていただく場合があります
件名	お問い合わせ件名を入力
お問い合わせ内容	お問い合わせ内容の本文を入力

※ 代理店経由のご契約の場合は、メール宛先「Cc」に代理店メールアドレスが追加されます

3.13. ドキュメント

3.13.1. サービスドキュメント

本サービスのドキュメントを掲載しています。

- 攻撃遮断くん サーバセキュリティタイプ サービス仕様書(本書)
- 攻撃遮断くん 導入マニュアル
- 攻撃遮断くん 利用マニュアル

3.13.2. FAQ

よくあるご質問(FAQ)を掲載しています。

3.13.3. お知らせ

本サービスからのお知らせを表示します。
お知らせには次の内容が掲載されます。

- お知らせ
- 機能追加
- メンテナンス情報
- 障害情報
- ルール更新
- セキュリティ情報

3.14. 設定制限値一覧

項目		ベーシックプラン	使い放題プラン	従量課金プラン
WAF設定	WAF設定（登録数）	契約数	300	300
	エージェント（登録数）	契約数	無制限 ※1	50
	信頼するIPリスト（登録数）	10000	10000	10000
	攻撃検知メール通知先（登録数）	20 / WAF設定	20 / WAF設定	20 / WAF設定
	カスタムルール（登録数） ※2 ※3	10 / WAF設定	10 / WAF設定	10 / WAF設定
	遮断時間（設定値）	60～3600	60～3600	60～3600
アカウント管理	ユーザー（登録数）	20	100	100
	グループ（登録数）	10	100	100
	ユーザーの所属組織数 ※4	50	50	50

※1 監視センターの負荷状況に応じ、監視センターのリソース増強を行う場合があります
※2 カスタムルールの登録はサポート窓口へお問い合わせください
※3 既存ルールの除外やアクション変更はカスタムルールに含まれません
※4 ユーザー（メールアドレス）は複数組織へ別々に登録が可能です

3.15. 代理店権限

本サービスは、アカウントに付与される権限により、操作可能な機能が異なります。
本節では、代理店権限別の操作内容について記載します。

3.15.1. 代理店用ユーザーアカウントの権限

代理店向けユーザーアカウントには、次の権限が付与されます。

項目	実行可能な操作
代理店	エンドユーザーのユーザーアカウント作成、グループ作成等、本サービスの主要管理機能に対する閲覧・登録・編集・削除の権限
代理店(閲覧)	エンドユーザーのユーザーアカウント作成、グループ作成等、本サービスの主要管理機能に対する閲覧権限

「代理店」権限については、当社でユーザーアカウントを初回発行する際に付与します。
代理店様にて作成いただくユーザーアカウントに対しては、「代理店 (閲覧) 」の付与が可能となります。

3.15.2. グローバルメニューの操作権限

機能	代理店	代理店(閲覧)
ユーザーの閲覧	◯※1	◯※1
ユーザーの追加 / 編集 / 削除	◯※1	✖
グループの閲覧	◯※1	◯※1
グループの追加 / 編集 / 削除	◯※1	✖

※1 管理対象企業(エンドユーザー)の機能のみが対象となります。

3.15.3. ユーザーメニューの操作権限

機能	代理店	代理店(閲覧)
ダッシュボード	◯※1	◯※1
分析ボード	◯※1	◯※1
攻撃ログ	◯※1	◯※1
レポート	◯※1	◯※1
WAF設定の閲覧	◯※1	◯※1
WAF設定の追加	◯※1	✖
WAF設定の編集 / 削除	◯※1	✖
監視エージェントの閲覧	◯※1	◯※1
監視エージェントの追加 / 編集	◯※1	✖
監視エージェントの削除	✖	✖
設定変更履歴の閲覧	✖	✖
請求情報の閲覧	◯※1	◯※1
契約情報の閲覧	◯※1	◯※1
プロフィール情報の閲覧 / 編集	◯	◯
マニュアル	◯	◯
サービス仕様書	◯	◯
FAQ	◯	◯
お問い合わせ	◯	✖

※1 管理対象企業(エンドユーザー)の機能のみが対象となります。

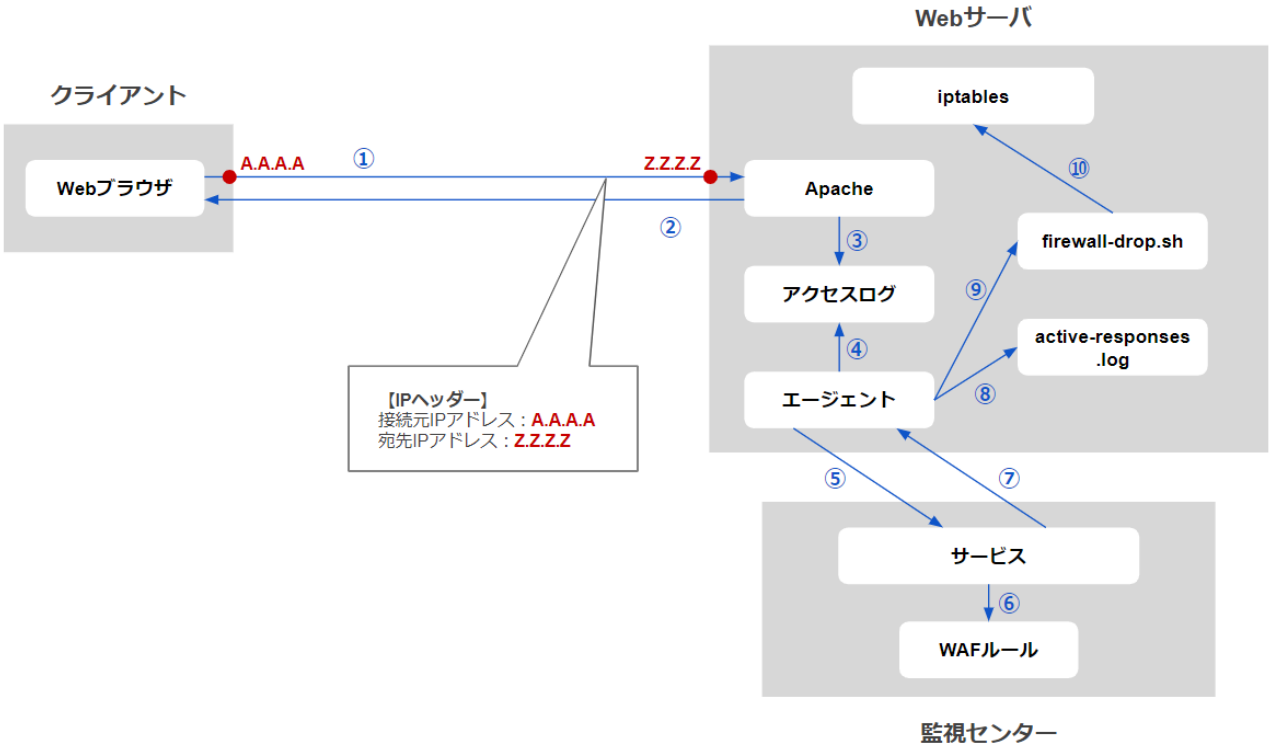
4. サービス技術仕様

本サービスで提供するWAFの技術仕様を記載します。

4.1. 遮断方式

攻撃検知後の遮断方式を記載します。

4.1.1. 通常遮断方式（iptables, Windows Firewall等）



① クライアントからWebサーバへHTTPリクエストを送信
② Webアプリケーション（Apache）がHTTPレスポンスを送信
③ Apacheがアクセスログを出力
④ エージェントがアクセスログを収集
⑤ エージェントが監視センターへログを送信（UDP通信）
⑥ ログをWAFセンタールールとシグネチャマッチング
⑦ 攻撃検知対象の場合は、エージェントへ遮断命令を送信
⑧ active-responses.logにログを出力
⑨ 遮断対象IPアドレスを引数にシェルスクリプトを起動
⑩ シェルスクリプトによりiptablesへ遮断ルールを追加（接続元IPアドレス：A.A.A.Aの拒否）

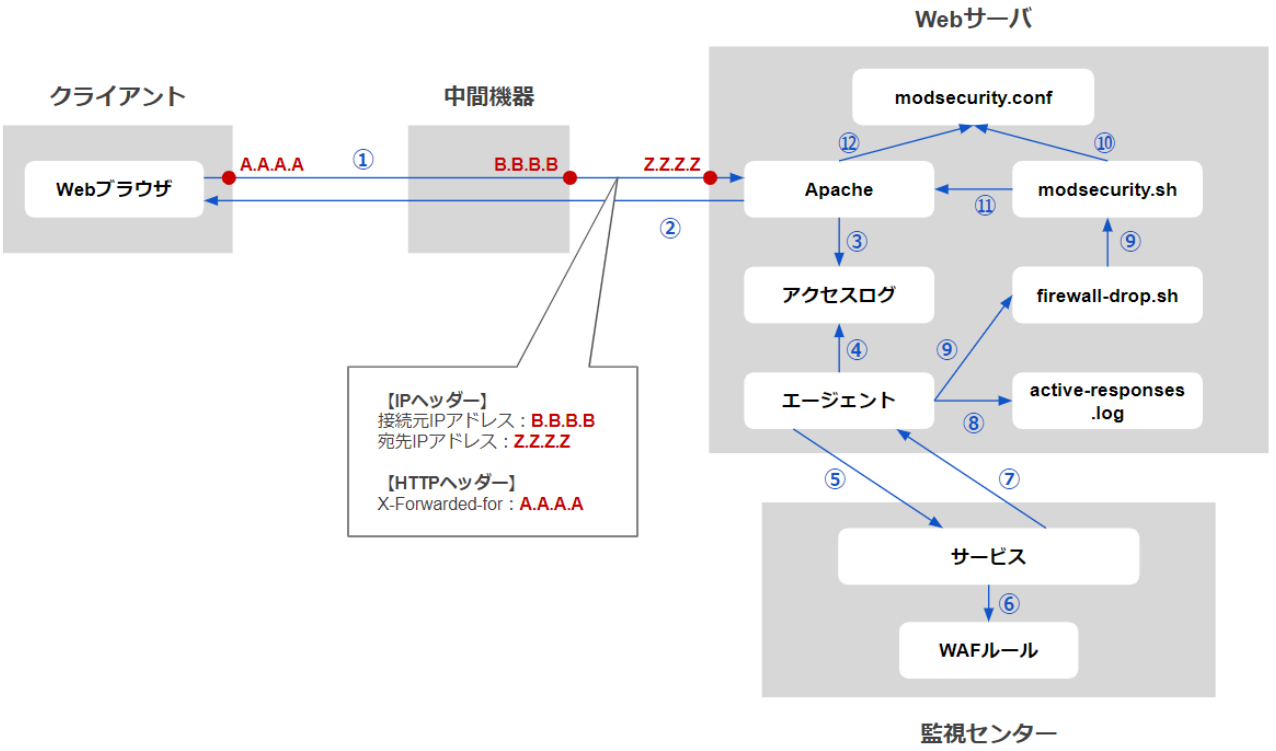
※遮断対象通信iptablesによりDropされます
※遮断時間（初期値：10分間）を経過した場合はシェルスクリプトにてiptablesから遮断ルールの削除が行われます

項目	内容
ルールIDとマッチングする情報	お客様にて設定したログ
遮断単位	IPアドレス単位
遮断時間	10分（初期値） ※約10分経過し、新たに攻撃がなければ解除
遮断時のクライアント画面 （クライアントのブラウザ画面）	タイムアウトエラー ※パケットdropされるため、クライアントのタイムアウト時間に達したら、エラー画面が表示されます（エラー画面の内容はクライアントにより異なります）

firewalld遮断の留意事項

WebアプリケーションでKeep-Aliveが有効の場合、複数リクエストが1コネクションで処理されます。firewalldではコネクション内の通信を許可するルールが攻撃遮断くんの遮断ルールより優先されます。
この動作によりfirewalldでは遮断処理が遅延する場合があります。本サービスではiptables遮断・nftables遮断のご利用を推奨します。

4.1.2. ModSecurity遮断方式



① クライアントからWebサーバへHTTPリクエストを送信
② Webアプリケーション（Apache）がHTTPレスポンスを送信
③ Apacheがアクセスログを出力
④ エージェントがアクセスログを収集
⑤ エージェントが監視センターへログを送信（UDP通信）
⑥ ログをWAFセンタールールとシグネチャマッチング
⑦ 攻撃検知対象の場合は、エージェントへ遮断命令を送信
⑧ active-responses.logにログを出力
⑨ 遮断対象IPアドレスを引数にシェルスクリプトを起動
⑩ シェルスクリプトによりmodsecurity.confへ遮断ルールを追加（X-Forwarded-for：A.A.A.Aの拒否）
⑪ シェルスクリプトによりApacheをリロード（graceful）
⑫ Apacheがmodsecurity.confを再読み込み

※遮断対象通信はApacheにより403ステータスで拒否されます
※遮断時間（デフォルト：10分間）を経過した場合はシェルスクリプトにてmodsecurity.confから遮断ルールの削除が行われます

項目	内容
ルール ID とマッチングする情報	お客様にて設定したログ
遮断単位	IPアドレス単位
遮断時間	10分（初期値） ※約10分経過し、新たに攻撃がなければ解除
遮断時のクライアント画面 （クライアントのブラウザ画面）	403エラー ※ 中間機器が403以外のエラーレスポンスを返す場合があります

Modsecurity遮断方式の留意事項

- Modsecurity遮断では、検知（遮断命令）のタイミングでWebアプリケーション（Apache / Nginx）のリロードを行います。検知頻度が多い場合、リロード処理の多発によりWebアプリケーションが不安定になる可能性があります。

- Modsecurity遮断方式をご利用の場合、ルール IDの採番は
「”固定値1（1桁）” ”時（2桁）” ”分（2桁）” ”秒（2桁）” ”ミリ秒（3桁）”」の 10桁です。

  ミリ秒以下で同時に検知処理を実施した場合には、次のように動作します。

  1. 遮断命令文に記述するルールIDが重複する場合があります。
  2. ルール IDが重複した場合、Apache / Nginx のリロードエラーをトリガーに一度削除処理が入り、その後再度リロード処理が行われます。ルールIDの重複が発生している限り、この処理が4度繰り返されます。

4.2. 防御対象の攻撃手法

本サービスで防御可能な攻撃を下表に例示します。

攻撃手法
● サーバサイドインクルードインジェクション ● HTTPインジェクション ● LDAPインジェクション ● XML外部エンティティ ● サーバサイドリクエストフォージェリ ● デシリアライゼーション ● クロスサイトスクリプティング ● SQLインジェクション ● NoSQLインジェクション ● OSコマンドインジェクション ● 改行コードインジェクション ● ディレクトリトラバーサル ● ファイルインクルード攻撃 ● URLエンコード攻撃 ● ブラックリストUA ● その他の WEB 攻撃全般 ● ミドルウェアなどの脆弱性を突いた攻撃（Apache Struts2の脆弱性等）

※ これらの攻撃に対し100%の防御を保証するものではございません

4.3. エージェント動作環境

Webサーバへ導入するエージェントプログラムの動作環境は次のとおりです。

項目	環境
CPU	Intel Pentium互換CPU 2コア以上
MEMORY	2GB以上
DISK	5GB以上の空き容量（ログの保存期間等による）

4.4. エージェント通信方式

4.4.1. 通信要件

IPv4のみ対応しています。

※IPv6通信の場合、遮断処理は行われません

4.4.2. 通信内容

エージェントから監視センターへに対して次の通信を行います。必要に応じてご利用環境のファイアウォール等を設定してください。

通信方向	対象	許可設定
送信（Out）	送信元IPアドレス	ご利用サーバIPアドレス
	宛先IPアドレス	監視センターIPアドレス
	送信元ポート（UDP）	ANY（1,024～65,535）
	宛先ポート（UDP）	監視センターポート番号

※ エージェントから監視センターへの通信はUDPで行われます
※ 送信元ポート番号はエージェント側でユニークに設定されます

4.5. エージェントの主要構成ファイル

項目	内容
/var/shadan-kun/etc/ossec.conf	エージェント設定ファイル
/var/shadan-kun/etc/client.keys	エージェントキー情報
/var/shadan-kun/logs/ossec.log	エージェント動作ログ
/var/shadan-kun/logs/active-responses.log	遮断動作ログ

※ エージェントインストール先が /var/shadan-kun の場合のファイルパスです
※ エージェントのログにローテーション機能はありません

4.6. 検査対象ログ

エージェントは、Webサーバに対して検査対象ログを監視センターへ送信し、攻撃の検知・遮断を行います。

4.6.1. 検査対象となるログ一覧

エージェントによる検査対象のログファイルを下表に例示します。

項目	内容
アクセスログ	/var/log/httpd/access_log
エラーログ	/var/log/httpd/error_log
システムログ	/varlog/messages
メールログ	/var/log/maillog
セキュリティログ	/var/log/secure

※ ファイルパスはOSやWebアプリケーションにより異なります（上記はCentOS + Apacheの例）

4.6.2. アクセスログフォーマット

本サービスでは、Webサーバのアクセスログを監視センターが解析します。
そのため、アクセスログは監視センターが解析可能なフォーマットにする必要があります。

【ログフォーマット例】

- Apache

```
"%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""
"%h %l %u %t \"%r\" %>s %b"
```

- Nginx

```
'$remote_addr - $remote_user [$time_local] "$request"' '$status $body_bytes_sent
$http_referer"' '"$http_user_agent";
```

- IIS

```
date time c-ip cs-username s-sitename s-computername s-ip s-port cs-method cs-uri-stem
cs-uri-query sc-status sc-win32-status sc-bytes cs-bytes time-taken cs-version cs(User-Agent)
cs(Cookie) cs(Referer)
```

※ オンラインエージェントの検知が正常に動作しない場合は「6.2. サポート窓口」まで
お問い合わせください（監視センター側でログデコーダのカスタマイズを実施いたします）

4.6.3. POSTデータの検査

本サービスでは、多様な攻撃から防御するためPOSTデータを検査対象とすることを推奨しています。POSTデータは「 **4.6.2.** アクセスログフォーマット」に出力することで、検査対象とすることが可能です。

※ 出力手順は管理画面のオンラインマニュアルを参照してください

4.7. ホスト・WAF設定単位の設定

本サービスでは、WAF 設定に対して対象ホスト 1 台で登録、または複数ホストを登録する等、柔軟な設定が可能です。

(例1) 1つのWAF設定に対して複数ホストを登録：
一定のWAF運用ルールと制御方針を複数台のWebサーバに適用する場合

(例2) 複数のWAF設定にホストを1台ずつ登録：
特定のWebサーバに対して「信頼するIPリスト」や「ルールカスタマイズ」等、個別の制御や設定で運用する場合

項目	内容
ホスト単位で設定可能	・検知モード / 遮断モードの切替
WAF設定単位で設定可能	・信頼するIPリスト ・防御証明メールのON/OFF ・防御証明メールの宛先設定 ・ルールカスタマイズ（シグネチャカスタマイズ） ・ログデコーダのカスタマイズ ・遮断時間の変更

4.8. シグネチャカスタマイズの種類

本サービスのシグネチャはご利用環境に応じてカスタマイズが可能です。

項目	内容
無効化	ルールIDを無効化
IPアドレス除外	ルールIDに対して特定のIPアドレスを除外
URI除外	ルールID（シグネチャ）に対して、特定のURIパスを除外
文字列除外	ルールIDに対して特定の文字列を除外
しきい値変更	しきい値が設定されたルールの変更 ※1
ルール追加	新規ルールを追加 ※1

※1 しきい値変更・ルール追加はサポート窓口へお問い合わせください

4.9. 動作環境

サポート対象**OS**

本サービスのエージェント動作を確認しているサーバOSおよびWebアプリケーションの一覧を記載します。動作確認範囲は次のとおりです。

1. エージェントインストール
2. 検知動作
3. 遮断動作

分類	サポート対象OS	Webアプリケーション	遮断方式
Windows	Windows Server 2012 R2 ※1	IIS8 ※2 , Apache ※3	Windows Firewall
Windows	Windows Server 2016 R2 ※1	IIS10 ※2 , Apache ※3	Windows Firewall
Windows	Windows Server 2019 ※1	IIS10 ※2 , Apache ※3	Windows Firewall
Windows	Windows Server 2022	IIS10 ※2 , Apache ※3	Windows Firewall
Windows	Windows Server 2025	IIS10 ※2 , Apache ※3	Windows Firewall
Linux	RedHat Enterprise Linux 6	Apache ※3 , Nginx ※4	iptables , modsecurity ※5
Linux	RedHat Enterprise Linux 7	Apache ※3 , Nginx ※4	iptables , modsecurity ※5 , firewalld ※7
Linux	RedHat Enterprise Linux 8	Apache ※3 , Nginx ※4	modsecurity ※5 , nftables ※6
Linux	RedHat Enterprise Linux 9	Apache ※3 , Nginx ※4	modsecurity ※5 , nftables ※6
Linux	RedHat Enterprise Linux 10	Apache ※3 , Nginx ※4	modsecurity ※5 , nftables ※6
Linux	CentOS 6	Apache ※3 , Nginx ※4	iptables , modsecurity ※5
Linux	CentOS 7	Apache ※3 , Nginx ※4	iptables , modsecurity ※5 , firewalld ※7
Linux	CentOS 8	Apache ※3 , Nginx ※4	modsecurity ※5 , nftables ※6
Linux	CentOS Stream 8	Apache ※3 , Nginx ※4	modsecurity ※5 , nftables ※6
Linux	CentOS Stream 9	Apache ※3 , Nginx ※4	modsecurity ※5 , nftables ※6
Linux	CentOS Stream 10	Apache ※3 , Nginx ※4	modsecurity ※5 , nftables ※6

Linux	Alma Linux 8	Apache※3 , Nginx※4	modsecurity※5 , nftables※6
Linux	Alma Linux 9	Apache※3 , Nginx※4	modsecurity※5 , nftables※6
Linux	Alma Linux 10	Apache※3 , Nginx※4	modsecurity※5 , nftables※6
Linux	Rocky Linux 8	Apache※3 , Nginx※4	modsecurity※5 , nftables※6
Linux	Rocky Linux 9	Apache※3 , Nginx※4	modsecurity※5 , nftables※6
Linux	Rocky Linux 10	Apache※3 , Nginx※4	modsecurity※5 , nftables※6
Linux	Ubuntu 16.04	Apache※3 , Nginx※4	iptables , modsecurity※5
Linux	Ubuntu 18.04	Apache※3 , Nginx※4	iptables , modsecurity※5
Linux	Ubuntu 20.04	Apache※3 , Nginx※4	iptables , modsecurity※5
Linux	Ubuntu 22.04	Apache※3 , Nginx※4	iptables , modsecurity※5
Linux	Ubuntu 24.04	Apache※3 , Nginx※4	iptables , modsecurity※5
Linux	Debian 10	Apache※3 , Nginx※4	iptables , modsecurity※5
Linux	Debian 11	Apache※3 , Nginx※4	iptables , modsecurity※5
Linux	Debian 12	Apache※3 , Nginx※4	iptables , modsecurity※5
Linux	Amazon Linux 2	Apache※3 , Nginx※4	iptables , modsecurity※5 , firewalld※7
Linux	Amazon Linux 2023	Apache※3 , Nginx※4	iptables , modsecurity※5
Linux	MIRACLE LINUX 8	Apache※3 , Nginx※4	iptables , modsecurity※5 , firewalld※7
Linux	MIRACLE LINUX 9	Apache※3 , Nginx※4	modsecurity※5 , firewalld※7

※1 Windows Server 2012 / 2016 / 2019 は Datacenter Editionで動作検証をしています
※2 OSバージョン毎のデフォルトIISバージョンで動作検証をしています
※3 OSバージョン毎に v2.2 , v2.4 のいずれかで動作検証をしています（Windows Server 2025の場合、Apache2.2 はサポート対象外です）

※4 OSバージョン毎に v1.14 , v1.16 , v1.21, v1.23 ～ v1.25 のいずれかで動作検証をしています
※5 OSバージョン毎に v2.7.3 , v2.9.0 ～ v2.9.3 ,v3.0.10 のいずれかで動作検証をしています
※6 v0.9.0 ～ v0.9.4 で動作検証をしています
※7 firewalld遮断の留意事項について「4.1.1. 通常遮断方式」を参照してください

サポート対象**OS**の**EOL**ポリシー

サポート対象OSがEOL（提供元ベンダーのサポート終了）を経過した場合におけるポリシーについて記載します。
OSのEOLについては、各ベンダーの公式Webサイトをご確認ください。

ベンダーサポートが終了したOSでは、開発・検証環境を用意することが困難となるため、弊社サポートがベストエフォートとなる場合があります。新規の脆弱性リスクに対応するため、弊社ではベンダーサポート期限内のOSをご利用いただくことを推奨しています。

弊社ではEOLを迎えたOSを使用しているお客様に対しても、可能な限りサポートを提供いたしますが、セキュリティおよび技術的な制約により、全ての問題に対して解決策を提供できるとは限らないことをご理解ください。

	EOL前	**EOL後**
動作実績	○	○※1
インストールパッケージ提供	○	○
質問への回答	○	○※2
トラブルシューティング対応	○	○※2
修正バッチ・スクリプト提供	○	○※3

※1 OSがEOL前に実施した動作検証やサポート実績を指します。
※2 OS起因による問題については解決策を提供できない場合があります。
※3 弊社提供のスクリプトやモジュールに不具合が確認された場合、ベストエフォートによる修正版の作成、検証を実施します。

4.10. 通知メール一覧

本サービスの通知メールは下表のとおりです。
通知メールは「アカウント」もしくは「WAF設定」登録のメールアドレス宛に送信されます。

通知条件	件名	内容	設定
お知らせ	※お知らせの内容により異なります	機能追加、障害情報、レポート公開、その他お知らせ等	アカウント
ログイン通知	[攻撃遮断くん] ログインしました	管理画面へのログイン	アカウント
エージェントキー発行	[攻撃遮断くん]新しいエージェントキーが発行されました	エージェントキー発行	WAF設定
エージェント接続状況の変化	[攻撃遮断くん] ご登録のエージェントの接続状況が変わりました	エージェントの接続状況がオンラインまたはオフラインに変化	WAF設定
攻撃検知メール	攻撃遮断くん攻撃検知メール - (host00XXXX) <IPアドレス> - 脅威レベル X	攻撃検知	WAF設定
月次レポート発行	[攻撃遮断くん] 月次レポートが発行されました: 20XX年XX月分	月次レポートのダウンロードURL	アカウント

4.11. 制限事項

- エージェントから監視センターへの通信はUDPプロトコルを利用します。プロトコルの性質上、通信経路で検査対象のログがDropする可能性があります（本サービスの監視センターではエージェントからの全ログを受信することを保証していません）。

- 本サービスの遮断処理は、監視センターに送信されたログを検査後、検知対象の送信元IPアドレスを遮断対象に登録します（IPアドレスベース遮断）。遮断対象に登録されるまでのリクエストは検知のみを実施します。

- エージェントと監視センター間のステータスが、オフラインからオンラインに変化した場合、オフライン期間のログ情報が監視センターへまとめて送信されます。一度に大量のログが送信された場合、しきい値系のシグネチャで検知/遮断される可能性があります。

- エージェントキーを複数台のWebサーバで重複利用することはできません。Webサーバごとにユニークなエージェントキーをご利用ください。

- ベーシックプランおよび従量課金プランのご利用において、特定エージェントのリクエストが多い場合、監視センターの負荷状況を考慮し、別監視センターへの移行をお願いすることがあります（Webサーバ側でエージェントキーの入れ替え作業が必要になる場合があります）。

- 使い放題プランのご利用において、監視センターの負荷状況に応じ、監視センターのリソース増強を行う場合があります。

この場合、監視センターサーバメンテナンスの際に一時的にWAF機能がご利用できなくなる場合があります。

5. 留意事項

- オフラインからオンラインにステータスが変化した際、オフライン期間中のログがまとめてお客様サーバーから監視センターに送信されます。この際、ログが一括送信されることにより、閾値系シグネチャで検知・遮断される場合がありますので、あらかじめご了承ください。遮断状態は通常、10分後に自動解除されます。
- Windows環境では、設定された遮断時間よりも実際の解除時間が数分長くなる場合があります。これは、Windowsのシステム処理や負荷状況、ファイアウォールの適用タイミングの影響によるものです。
- サーバセキュリティタイプの仕様上、検知から遮断までにタイムラグが発生します。そのため、最初のリクエストは検知のみとなることをご了承ください。
- サーバセキュリティタイプでは、エージェントが送信するログをCSC監視センターへ転送する際にUDPを使用します。このため、通信経路上でログがドロップされる可能性があり、CSC監視センターにおいて100%の受信を保証するものではありません。
- ModSecurityにより遮断が発生すると、遮断命令が書き込まれるたびにApache/nginxのリロードが実行されます。そのため、攻撃頻度が高い場合、短期間にリロードが頻発し、Webアプリケーションが不安定になる可能性があります。
- ベーシックプラン/従量課金プランの留意事項

  1サービスあたり、秒間200リクエスト（月間5億2000万リクエスト）を超える場合、監視センターの負荷状況に応じて別の監視センターへの移行をお願いすることがあります。移行が必要な場合、お客様によるエージェントの再インストールが求められる場合があります。
- 使い放題プランの留意事項

  監視センターの負荷状況に応じてリソース増強を実施する場合があります。その際、一時的にWAF機能がご利用いただけなくなる可能性があります。

6. サービス窓口

6.1. サポート問い合わせ

本サービスをご利用いただくにあたり、技術的な問い合わせ窓口として「サポート窓口」をご用意しております。

項目	内容
サポート窓口	1. メールサポート（平日 9:00-18:00） ● 管理画面：「お問い合わせ」メニュー ● メールアドレス：support@cscloud.co.jp 2. 電話サポート（24時間365日） ● 電話番号：03-6416-1580 ○ 営業時間外（平日 9:00-18:00以外）は、トラブル等の緊急対応の電話受付を実施しています ○ 050-3185-3318もしくは070/080/090番号より担当者からご連絡する場合があります
提供範囲	● FAQおよび仕様確認に対する問い合わせ ● 管理画面の操作に関するサポート ● ご提供マニュアルに沿った設定サポート ● 各種設定サポート ● シグネチャカスタマイズ ● トラブルシューティング
応答時間	ベストエフォート
対応言語	日本語
障害発生時の通知方法	● 特定ユーザーのみに影響がある場合： 個別に障害発生をご連絡（メールもしくはお電話） ● 特定プランの全ユーザーに影響がある障害： 管理画面のお知らせより障害発生を通知 ※個別にご連絡をさせていただく場合もあります

6.2. 契約関連問い合わせ

契約に関するお問い合わせは、販売代理店または営業窓口までご連絡ください。

- 新規のご契約
- 導入前のお問い合わせ
- 契約内容の変更
- 請求先情報の変更
- 企業名の変更
- 解約

【営業窓口】
受付時間　：平日 9:00 - 18:00
電話番号　：03-6416-1579
Email　：sales@cscloud.co.jp